UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/505,951	02/15/2000	Simon Robert Walmsley	AUTH08US	5608

7590 01/18/2006

Kia Silverbrook
Silverbrook Research Pty Ltd
393 Darling Street
Balmain, 2041
AUSTRALIA

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 01/18/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/505,951	WALMSLEY ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 November 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. A response was received on 03 November 2005. No claims have been amended, added, or canceled. Claims 1-20 are currently pending in the present application.

Response to Arguments

2. Applicant's arguments filed 03 November 2005 have been fully considered but they are not persuasive.

Claims 1-4, 6-15, and 17-20 were rejected under 35 U.S.C. 103(a) as unpatentable over Sony Corporation (Kusakabe), European Patent EP 0817420, in view of Spies et al, US Patent 5689565. Claims 5 and 16 were rejected under 35 U.S.C. 103(a) as unpatentable over Sony in view of Spies, and further in view of Schneier, *Applied Cryptography*.

The Examiner notes that Applicant's response is not considered to be fully responsive under 37 CFR 1.111(b). Specifically, Applicant's reply must reply to every ground of objection and rejection in the prior Office action, and must present arguments pointing out the specific distinctions believed to render the claims, including any newly presented claims, patentable over any applied references. Applicant has not replied to the rejections of Claims 2-20 under 35 U.S.C. 103(a) and has not presented any arguments specifically in reference to Claims 2-20. However, given the dependences

and the correspondence between the Claims, the Examiner has considered the present response to be a *bona fide* attempt to advance the prosecution of the present application; therefore, the present response and the arguments therein have been considered as set forth below.

In reference to Claim 1, in response to applicant's argument that Spies is nonanalogous art to Sony, it has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, Applicant argues that Sony is concered with authenticating IC cards, whereas Spies is concerned in particular with encrypting and decrypting a document. However, the Examiner notes that encryption and decryption are clearly part of the authentication method of Sony (see column 9) and that Spies explicitly discloses authentication functionality (see column 1, lines 7-11, the "Technical Field" of the invention). Therefore, the Examiner believes that the references should clearly be considered as analogous art.

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Specifically, Applicant argues that Sony describes the use of random numbers but does not describe the use of signatures, and that Spies describes computing the hash of a document and does not describe the use of random numbers (page 2, paragraph 1 of the present response). The Examiner agrees with Applicant's assertion that the Examiner previously explicitly stated that Sony does not describe the use of signatures; however, Sony was not relied upon to teach such a limitation. Instead, Spies was relied upon to teach the use of signatures. Regarding the assertion that Spies does not describe the use of random numbers, the Examiner respectfully disagrees, noting that Spies clearly discloses uses of random numbers (see column 9, lines 30-33, for example, where a key is randomly selected). Further, Applicant further asserts that the document described in Spies cannot be a random number because it is "constructed" or "selected". However, the Examiner first notes that the terms "construct" and "select" do not exclude random construction or selection. The Examiner further notes that Spies was not relied on to explicitly disclose signing of a random number and encryption of the number and signature, but rather for a more general teaching of digitally signing something in general and encrypting the signed object together with the signature.

In response to applicant's argument that "a combination of Sony and Spies would describe generating a random number and encrypting the random number with a key, computing the hash of a document (and instrument) through the use of a hashing algorithm, encrypting the hash using an asymmetric key, encrypting the document and added hash with a symmetric key, then forwarding the encrypted random number, and

encrypted hash function and document, where the random number and the encrypted hash function and document are encrypted with two different keys" (see page 3, paragraph 1 of the present response), the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981). Applicant's proposed combination, quoted above, is mere speculation, and would result only from naïvely combining all of the limitations recited. Instead, Spies was relied upon for the general teaching of the use of a signature of a general "document" and encrypting both the document and the signature under the same symmetric key (Spies, column 12, lines 6-27) for the purpose of authenticating the sending of the document (Spies, column 13, lines 26-32). To one skilled in the art considering the authentication method disclosed by Sony and the above teaching of Spies, it would have been obvious to use a signature of the random number in Sony to further provide authentication of the random number, as taught by Spies. Regarding Applicant's further assertion that the combination of Sony and Spies would not teach the random number and signature being enciphered by the same key, the Examiner believes that it would further have been obvious to use the same key that already encrypts the random number in Sony for also encrypting the signature, as in Spies.

Applicant further argues that neither Sony nor Spies describe encrypting the decrypted random number with a second symmetric key and returning it to the "trusted authentication chip" (page 3 of the present response). However, the Examiner notes that Sony clearly discloses re-encrypting the decrypted random number with a second symmetric key and returning it to the first device (Sony, column 9, lines 41-48; column 9, line 57-column 10, line 2; Figures 7-9).

Applicant additionally argues that neither Sony nor Spies describe the steps of encrypting the random number using the second key in the trusted chip, comparing the two random numbers encrypted using the second key in the trusted chip, and considering the untrusted chip to be valid or invalid based on whether the two random numbers match (bottom of page 3 of the present response). However, this amounts to a general allegation because the arguments do not specifically point out differences between the claim limitations and the cited prior art. The Examiner believes that Sony does disclose that the encrypted random number is compared with the originally encrypted random number (column 10, lines 29-31) after first being decrypted with the symmetric decryption function using the second key (column 10, lines 21-28), and the two numbers matching authenticates the second apparatus (column 10, lines 31-35) and the two numbers not matching does not authenticate the second apparatus (column 10, lines 36-39). The Examiner notes that although Sony discloses decrypting the encrypted random number while the claim recites encrypting the random number, because the encryption function is a symmetric encryption function, the encryption and decryption functions are equivalent because they use the same key and algorithm.

Therefore, the comparison of the two numbers gives the same result and is not patentably distinct.

Therefore, for the reasons detailed above, the Examiner maintains the rejection as set forth below.

Terminal Disclaimer

3. The terminal disclaimer filed on 03 November 2005 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of Patent No. 6,816,968 has been reviewed and is accepted. The terminal disclaimer has been recorded.

Double Patenting

4. The rejection of Claims 1-9, 11, and 14-19 under the doctrine of obviousness-type double patenting as unpatentable over Claims of US Patent 6816968 is withdrawn in light of the above-mentioned terminal disclaimer.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-4, 6-15, and 17-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sony Corporation (Kusakabe), European Patent EP 0817420, in view of Spies et al, US Patent 5689565.

In reference to Claim 1, Sony discloses an authentication method (see Figures 7-9, Claim 1, and column 2, line 49-column 3, line 17) in which a random number is generated (column 8, lines 12-17) and encrypted with a symmetric encryption function using a first key in a first apparatus (column 9, lines 13-17). The encrypted random number is sent to a second apparatus (column 9, lines 18-21) and decrypted with a symmetric decryption function using the first key (column 9, lines 31-37), and then encrypted with the symmetric encryption function using a second key (column 9, lines 41-48) and sent to the first apparatus (column 9, line 57-column 10, line 2). The encrypted random number is compared with the originally encrypted random number (column 10, lines 29-31) after first being decrypted with the symmetric decryption function using the second key (column 10, lines 21-28). The two numbers matching authenticates the second apparatus (column 10, lines 31-35) and the two numbers not matching does not authenticate the second apparatus (column 10, lines 36-39). However, Sony does not disclose the calculation and comparison of a digital signature as a step of the authentication method.

Spies discloses a cryptographic system and method that includes generating a digital signature of a document (column 12, lines 6-13) and encrypting the document

and digital signature under the same symmetric encryption key in a sending device (column 12, lines 14-27, noting especially the equation at line 25). Spies further discloses decrypting the document and signature at a receiving device (column 13, lines 15-22) and verifying the signature (column 13, lines 20-36). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Sony by including the steps of generating a digital signature of the random number (the "document") and encrypting the signature with the random number in the first apparatus, and of decrypting and verifying the signature in the second apparatus, in order to authenticate the sending of the random number (see Spies, column 13, lines 26-32) and more generally to allow for greater security, privacy, authenticity, and integrity in the system (see Spies, column 2, lines 1-4).

In reference to Claim 2, Sony and Spies further disclose that the first and second keys are held in both the first and second apparatuses (see Sony, Figure 9).

In reference to Claim 3, Sony and Spies further disclose that the first apparatus contains a random function to generate random numbers (see Sony, column 8, lines 12-15).

In reference to Claim 4, Sony and Spies further disclose that the second apparatus holds a decryption function (see Sony, column 9, lines 31-37).

In reference to Claim 6, Sony and Spies further disclose that the second apparatus decrypts the random number with the first key (see Sony, column 9, lines 31-37), encrypts the random number with the second key (Sony, column 9, lines 41-48), and sends the encrypted random number to the first apparatus (Sony, column 9, line

57-column 10, line 2). Additionally, Sony and Spies further disclose verifying the signature in the second apparatus (see Spies, column 13, lines 20-36).

In reference to Claim 7, Sony and Spies further disclose that the second apparatus monitors the time elapsed between steps of its processing (see Sony, column 10, lines 53-56).

In reference to Claim 8, Sony and Spies further disclose that the function generating the random numbers is held in the first apparatus (see Sony, column 8, lines 12-15). Additionally, Sony and Spies disclose that if the second apparatus is not authenticated, the authentication process is terminated (Sony, column 10, lines 36-39).

In reference to Claim 9, Sony and Spies further disclose that the first apparatus monitors the time elapsed between steps of its processing (see Sony, column 10, lines 6-7).

In reference to Claim 10, Sony and Spies further disclose that it is determined if the second apparatus is valid (see Sony, column 10, lines 31-35) or not (Sony, column 10, lines 36-39).

Claims 11-15 and 17-20 are system claims reciting limitations corresponding substantially to those of the methods of Claims 1-4 and 6-10, and are thus rejected by a similar rationale.

7. Claims 5 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sony in view of Spies as applied to claims 1 and 11 above, and further in view of Schneier, *Applied Cryptography*.

Sony as modified by Spies discloses everything as applied to Claims 1 and 11 above. However, Sony does not disclose the use of digital signatures, and Spies does not explicitly disclose the use of digital signatures of 160 bits. Schneier discloses that hash functions can be used in the creation of digital signatures, and specifically discloses the use of 160 bit hashes (page 38, last paragraph). Therefore, it would have been obvious to modify the method of Sony and Spies to include digital signatures 160 bits in length in order to increase the speed of the signature algorithm (see Schneier, page 38, last paragraph-page 39, first full paragraph).

Conclusion

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER